IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicant | : David P. Cook | Art Unit | : 2137 |
| Serial No. | : 10/616,100 | Examiner | : Minh Dieu T. Nguyen |
| Filed | : July 8, 2003 | Conf. No. | : 1883 |
| Title | : SECURE MESSAGE FORWARDING SYSTEM DETECTING USER'S PREFERENCES INCLUDING SECURITY PREFERENCES | | |

**Mail Stop Appeal Brief - Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

Applicant files this brief on appeal under 37 C.F.R. § 41.37, in response to the Notice of Panel Decision from Pre-Appeal Brief Review mailed April 14, 2008 and to the Notification of Non-Complaint Appeal Brief mailed May 20, 2008.

The section required by 37 CFR § 41.37 follows.

**(1) Real Party in Interest**

The case is assigned of record to Zix Corporation, a corporation of Dallas, Texas, who is the real party in interest.

**(2) Related Appeals and Interferences**

There are no related appeals or interferences.

**(3) Status of Claims**

Claims 1-92, 95-96 and 108-139 were canceled during prosecution. Only claims 93-94 and 97-107 are pending, with claims 93, 97, 100 and 106 being independent. Applicant appeals the rejection of claims 93-94 and 97-107.

**(4) Status of Amendments**

There are no unentered amendments.

## (5) Summary of Claimed Subject Matter

**Claim 93**

| Claim Language | Support in Specification and/or FIGS. |
|---|---|
| A computer implemented method for sending a secure message to multiple recipients comprising: | *See e.g.*, Fig. 6. |
| encrypting a message; | *See e.g.*, page 16, line 20 to page 17, line 1; page 21, lines 8-11; page 23, line 23 to page 24, line 1. |
| sending the encrypted message to a forwarding server, including providing a list of recipients to the forwarding server; | *See e.g.*, page 26, line 23 to page 27, line 2; *see also* operations 307, 314 and 319 in Fig. 2(c) and forwarding service 195 and forwarding engine 198 in Fig. 1a-1. |
| at the forwarding server, decrypting the encrypted message and determining a delivery preference for each recipient in the list of recipients; and | *See e.g.*, page 15, line 25 to page 16, line 2; page 35, lines 3-13; page 36, lines 24-25; and page 37, line 25 to page 38, line 3. |
| for each recipient that has a delivery preference, re-encrypting the message and delivering the re-encrypted message in accordance with the delivery preference. | *See e.g.*, page 14, lines 3-7; page 17, lines 2-5 and 10-12; and page 38, lines 3-10. |

**Claim 97**

| Claim Language | Support in Specification and/or FIGS. |
|---|---|
| A computing system for providing secure message services for messages addressed to multiple recipients, comprising: | *See e.g.*, Figs. 1a, 1a-1 and 1a-2 and 6. |
| a forwarding engine executing on a computer operable to: | *See e.g.*, forward engine 198 of forwarding service 195 in Fig. 1a-1; *see also* page 13, lines 21-24. |
| receive an encrypted message and a list of recipients; | *See e.g.*, page 16, line 20 to page 17, line 1; page 21, lines 8-11; page 23, line 23 to page 24, line 1. |
| decrypt the encrypted message; | *See e.g.*, page 35, lines 4-11 and page 36, lines 24-25. |
| determine a delivery preference for each recipient in the list of recipients; | *See e.g.*, operation 605 in Fig. 6. |
| for each recipient that has a delivery preference, re-encrypt the message and deliver the re-encrypted message in accordance with the delivery preference; and | *See e.g.*, page 15, line 25 to page 16, line 1; page 17, lines 10-12; and page 38, lines 6-10. |
| for each recipient that does not have a delivery preference, notify the recipient that the message is available for retrieval. | *See e.g.*, Fig. 2e; *see also* page 17, lines 7-10; page 21, lines 15-18; and page 38, lines 11-17. |

**Claim 100**

| Claim Language | Support in Specification and/or FIGS. |
|---|---|
| A computer implemented method for sending a secure message to multiple recipients comprising: | *See e.g.*, Fig. 6. |
| encrypting a message; | *See e.g.*, page 16, line 20 to page 17, line 1; page 21, lines 8-11; page 23, line 23 to page 24, line 1. |
| sending the encrypted message to a forwarding server, including providing a list of recipients to the forwarding server; | *See e.g.*, page 26, line 23 to page 27, line 2; *see also* operations 307, 314 and 319 in Fig. 2(c) and forwarding service 195 and forwarding engine 198 in Fig. 1a-1. |
| at the forwarding server, decrypting the encrypted message and determining a decryption capability for each recipient in the list of recipients; and | *See e.g.*, page 15, line 25 to page 16, line 2; page 17, lines 3-13; and page 18, lines 12-16. |
| for each recipient, re-encrypting the decrypted message according to the decryption capability of the recipient and delivering the re-encrypted message to the recipient. | *See e.g.*, page 17, lines 10-16; page 18, line 21 to page 19, line 1; and page 21, lines 11-14. |

**Claim 106**

| Claim Language | Support in Specification and/or FIGS. |
|---|---|
| A computing system for providing secure message services for messages addressed to multiple recipients, comprising: | *See e.g.*, Figs. 1a, 1a-1 and 1a-2 and 6. |
| a forwarding engine executing on a computer operable to: | *See e.g.*, forward engine 198 of forwarding service 195 in Fig. 1a-1; *see also* page 13, lines 21-24. |
| receive an encrypted message and a list of recipients; | *See e.g.*, page 16, line 20 to page 17, line 1; page 21, lines 8-11; page 23, line 23 to page 24, line 1. |
| Decrypt the encrypted message; | *See e.g.*, page 35, lines 4-11 and page 36, lines 24-25. |
| for each recipient in the list of recipients, determine whether the recipient has a decryption capability; | *See e.g.*, page 15, line 25 to page 16, line 2; page 17, lines 3-13; and page 18, lines 12-16. |
| for each recipient with a decryption capability, re-encrypt the message according to the decryption capability of the recipient and | *See e.g.*, page 17, lines 10-16; and page 18, line 21 to page 19, line 1 |

| | |
|---|---|
| deliver the re-encrypted message to the recipient; and | |
| for each recipient that does not have a decryption capability, notify the recipient that the message is available for retrieval. | *See e.g.*, page 17, lines 7-10; and page 21, lines 15-17. |

**(6) Grounds of Rejection to be Reviewed on Appeal**

Claim 93 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over USP No. 6,343,327 to **Daniels** in view of USP No. 7,051,003 to **Kobata**.

Claims 94 and 97-99 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over **Daniels** in view of **Kobata**, and further in view of USP No. 6,023,700 to **Owens**.

Claims 100 and 103-105 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over **Daniels** in view of **Kobata**, and further in view of USP No. 6,697,944 to **Jones**.

Claims 101-102 and 106-107 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over **Daniels** in view of **Kobata** and **Jones**, and further in view of USP No. 6,865,191 to **Bengtsson**.

These grounds of rejection are requested to be reviewed on appeal.

**(7) Argument**

**Section 103(a) Rejections**

Claim 93 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over **Daniels** in view of **Kobata**. Applicant respectfully traverses this rejection.

**A. Daniels' forwarding server does not determine a delivery preference for each recipient**

Claim 93 recites in part **determining by the forwarding server a delivery preference for each recipient** in the list of recipients.

In the Office Action dated September 10, 2007 ("Final Office Action"), the Examiner, citing col. 6, lines 66-67, maintained that Daniels provides these features because Daniels'

"message router 112 decodes the delivery preference data" for each recipient. *See* page 5, item 5, lines 13-15 of Final Office Action.

Applicant respectfully submits that Daniels' delivery preferences for the recipients are not determined by the message router 112. Rather, Daniels' sender 100 determines the delivery preference information for each recipient (e.g., from sender's customer database 202 shown in Fig. 2) at the time of submitting the documents to Daniels' printstream processor 102 for processing and delivery. Daniels' message router 112 merely functions to route the message to an appropriate channel using delivery preference data that has already been determined in advance prior to forwarding the data to the message router 112. For at least this reason, Applicant respectfully asserts claim 93 is allowable over Daniels.

**B. Daniels' forwarding server does not decrypt an encrypted message**

Claim 93 further recites in part a forwarding server that **decrypts an encrypted message**.

In the Final Office Action dated September 10, 2007 ("Final Office Action"), the Examiner suggested that Daniels' message router 112 operates to decrypt an encrypted message. *See*, page 5, item 5, lines 8-9 of Final Office Action. Applicant respectfully disagrees, and submits that Daniels' message router 112 does not provide any decryption capability for decrypting an encrypted message. At most, Daniels shows decoding a portion of a message (e.g., the preference portion), but does not "decrypt" the message. Applicant respectfully submits that decoding a message is not the same as decrypting a message. The Examiner even conceded this distinction that Daniels is "silent on the capability of decrypting an encrypted message at the forwarding server." *See*, page 3, lines 1-3 of Final Office Action.

**C. Daniels' forwarding server does not deliver a re-encrypted message in accordance with delivery preference**

Claim 93 further recites in part re-encrypting a message and **delivering the re-encrypted message in accordance with the delivery preference**. Applicant reiterates that Daniels' message router 112 has no decryption capability. Daniels' message router 112 also does not "re-encrypt" a message. Accordingly, Daniels provides no teaching or suggestion of delivering a re-

encrypted message in accordance with delivery preferences of a recipient. The Examiner conceded that Daniels does not teach or suggest re-encrypting a message. *See*, page 6, lines 6-7 of Final Office Action.

Kobata does not remedy the deficiencies of Daniels. The Examiner asserted that Kobata's server system decrypts a parcel, re-encrypts the parcel and delivers the re-encrypted parcel. *See*, page 6, lines 7-9 of Final Office Action. Even assuming for the sake of argument (a point Applicant does not concede) that Kobata decrypts an encrypted parcel, re-encrypts the parcel and delivers the re-encrypted parcel as suggested by the Examiner, the proposed combination of Daniels and Kobata still does not arrive at the claimed invention because neither Daniels nor Kobata provide any teaching or suggestion of delivering a re-encrypted parcel in accordance with a delivery preference. The absence of a delivery preference is further supported by the fact that Kobata's server system 26 does not deliver the encrypted parcel. Rather, the parcel is manually retrieved by the receiving system 18 (10:35-48). Because Kobata's receiving system manually retrieves the parcel (e.g., by logging onto the server system 26), a delivery preference is not necessary.

For at least these reasons, Applicant respectfully submits that the proposed combination of Daniels and Kobata does not render claim 93 obvious.

## Section 103(a) Rejections

Claim 94 and 97-99 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over **Daniels** in view of **Kobata**, and further in view of **Owens**. Applicant respectfully traverses this rejection.

### A. Daniels' forwarding server does not notify a recipient that a message is available for retrieval

Claim 97 recites in part a forwarding engine operable to **notify** the recipient that a message is available for **retrieval** for **each recipient that does not have a delivery preference**. The Examiner pointed out Daniels' col. 4, lines 18-23, Kobata's col. 5, lines 43-46, and Owens' col. 4, lines 18-20, col. 5, lines 37-44 and col. 6, lines 52-55 as allegedly disclosing these

claimed features. *See*, page 3, lines 6-17 of Final Office Action. Applicant will now address each section below.

Daniels' col. 4, lines 18-23 is directed to sending electronic mail pieces to the message router 112 for delivery in accordance with the addressing information (e.g., to a web server 116, electronic mail address, pager, fax number, etc.). Nowhere in this section does Daniels' provide any teaching or suggestion of notifying a recipient in an event that the recipient does not have a delivery preference. In fact, by providing the various addressing information, Daniels' does not contemplate the situation in which a recipient does not have delivery information. Daniels also does not notify a recipient that a mail piece is available for retrieval if a delivery preference has not been defined. Each mail piece is sent out to the recipient by the output server 113. There is nothing in Daniels that suggests that the output server 113 notifies a recipient that a mail piece is available for retrieval.

Kobata's col. 5, lines 43-46 is directed to sending, by the sending system 14, a notification to the receiving system 18 that a parcel intended for the receiving system 18 is in route to the server system 26, where the parcel can be retrieved. *See also* 5:54-56. Kobata's sending system 14 notifies the receiving system 18 of the parcel in transit regardless of whether the receiving system 18 has or does not have a delivery preference.

Owens' col. 4, lines 18-20 provides that a user may dial into an email mailbox with a computer and playback voice mail messages, view fax mail mesages and read email messages. Owens' col. 6, lines 52-55 provides that after messages arrive at the designated service (e.g., electronic mail service or telecommunications service), the messages may be sent to or stored in mailboxes associated with the individual message receivers for later retrievel by the receiver. Nowhere in these sections does Owen consider recipients that do not have a delivery preference and notify such recipients that messages are available for retreival. Rather, Owens' teaches away from Applicant's claimed notification specifically providing (*see, e.g.,* Owens' col. 5, lines 37-44) the option of forwarding an electronic message to the receiver's mailbox if the message receiver does not specify a preference for receiving an incoming message, rather than notifying the recipient that the message is available for retrieval.

For at least these reasons, Applicant respectfully submits that the proposed combination of Daniels, Kobata and Owens does not render claim 97 obvious. Claim 98 depends from claim

97, and also is submitted to be allowable for at least the same reasons discussed above with respect to claim 97.

Claims 94 and 99 depend from claim 93, and also are allowable for at least the same reasons discussed above with respect to claim 93.

## Section 103(a) Rejections

Claim 100 and 103-105 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over **Daniels** in view of **Kobata**, and further in view of **Jones**. Applicant respectfully traverses this rejection.

### A. The proposed combination does not determine a decryption capability for each recipient

Claim 100 recites in part at the forwarding server, **determining a decryption capability for each recipient in the list of recipients**.

The Examiner admitted that Daniels does not teach or suggest these features, and relies upon col. 2, lines 40-46 of Kobata to cure these deficiencies. *See*, page 10, line 19 to page 11, line 6 of Office Action.

Applicant respectfully submits that the relied upon section of Kobata only provides an encryption-decryption process for sending a parcel. However, Kobata does not teach or suggest determining an encryption capability for each recipient and encrypting a parcel based on a recipient's decryption capability.

### B. The proposed combination does not re-encrypt a decrypted message according to a decryption capability of a recipient and deliver the re-encrypted message

Claim 100 further recites in part **re-encrypting the decrypted message according to the decryption capability of the recipient** and **delivering the re-encrypted message** to the recipient. The Examiner acknowledged that neither Daniels nor Kobata teach or suggest these features, but relies on col. 4, lines 30-35 of Jones to cure these deficiencies. *See*, page 11, lines

12-19 of Final Office Action. Applicant respectfully disagrees.

Jones describes that the digital content provider 60 may interrogate a user's device 64 to determine the level at which the device 64 is to be trusted with digital content (e.g., music files) so as to limit the user's ability to engage in illegal redistribution of the content (8:53-58). The provider 60 may use the user's public key to encrypt the digital content such that its playback could only be effectuated by the user's device 64 by decrypting the digital content with its private key during playback (8:62-65).

Applicant respectfully submits that while Jones checks the trust level of the user device 64, Jones does not determine the decryption capability of the user device 64. The relied upon portion of Jones does not discuss how decryption capability is determined. Applicant respectfully submits that determining the trust level of a device is wholly distinct from determining the decryption capability of the device, as the determination of the device's trust level relates to authorization while the determination of the device's decryption capability relates to enablement once the trust level has been determined. For at least these reasons, Applicant respectfully submits that the proposed combination of Daniels, Kobata and Jones does not render claim 100 obvious.

Claims 103-105 depend from claim 100, and also are allowable for at least the same reasons discussed above with respect to claim 100.

**Section 103(a) Rejections**

Claim 101-102 and 106-107 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over **Daniels** in view of **Kobata** and **Jones**, and further in view of **Bengtsson**.

**A. The proposed combination does not determine (1) whether a recipient has a decryption capability for each recipient, (2) re-encrypt the message according to the decryption capability of the recipient, and (3) notify the recipient that the message is available for retrieval.**

Claim 106 recites in part a forwarding engine operable to **determine whether the recipient has a decryption capability** for each recipient in the list of recipients, **re-encrypt the message according to the decryption capability of the recipient** for each recipient with a

decryption capability, and **notify the recipient that the message is available for retrieval** for each recipient that does **not** have a decryption capability.

The Examiner previously admitted that neither Daniels, Kobata nor Jones teach or suggest these features. *See*, page 14, line 21- page 15, line 5 of First Office Action. To cure these deficiencies, the Examiner relies upon Bengtsson's col. 5, lines 22-34 and lines 43-55 (and col. 6, lines 60-67), alleging that Bengtsson's server 32 can deliver sender's SMS message and attachment in a format that can be deciphered by the receiver terminal 34 if the receiver terminal 34 does not have the capability to decipher the SMS message and attachment. *See*, page 4, line 18- page 5, line 3 of Final Office Action. Applicant respectfully submits that reformatting a message so that the message can be deciphered by the receiver terminal 34 does not mean that the message is being encrypted or re-encrypted according to the receiver terminal's decryption capability. In fact, Bengtsson describes that the SMS attachment may be accessed as an ordinary HTML file if the receiver terminal 34 cannot decipher the attachment, evidencing that the message is being reformatted according to a format compatibility, not decryption capability, of the receiver terminal 34.

For at least these reasons, Applicant respectfully submits that the proposed combination of Daniels, Kobata, Owens and Bengtsson does not render claim 106 obvious. Claim 107 depends from claim 106, and is allowable for at least the same reasons discussed above with respect to claim 106.

Claims 101 and 102 depend from claim 100, and also are allowable for at least the same reasons discussed above with respect to claim 100.

No fee is believed to be due. If necessary to keep the pending appeal brief active and pending, please apply charges (or credits) to Deposit Account No. 06-1050.

Respectfully submitted,

Date: June 18, 2008

/Alex Chan/
Alex Chan
Reg. No. 52,713

Customer No. 26181
Fish & Richardson P.C.
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

50492367.doc

## Appendix of Claims

93. A computer implemented method for sending a secure message to multiple recipients comprising:

encrypting a message;

sending the encrypted message to a forwarding server, including providing a list of recipients to the forwarding server;

at the forwarding server, decrypting the encrypted message and determining a delivery preference for each recipient in the list of recipients; and

for each recipient that has a delivery preference, re-encrypting the message and delivering the re-encrypted message in accordance with the delivery preference.

94. The computer implemented method of claim 99, wherein:

notifying the recipient includes notifying the recipient that the message is available for retrieval through a secure link.

97. A computing system for providing secure message services for messages addressed to multiple recipients, comprising:

a forwarding engine executing on a computer operable to:

receive an encrypted message and a list of recipients;

decrypt the encrypted message;

determine a delivery preference for each recipient in the list of recipients;

for each recipient that has a delivery preference, re-encrypt the message and deliver the re-encrypted message in accordance with the delivery preference; and

for each recipient that does not have a delivery preference, notify the recipient that the message is available for retrieval.

98. The computing system of claim 97, wherein the forwarding engine is operable to:

notify the recipient that the message is available for retrieval through a secure link.

99. The computer implemented method of claim 93, further comprising notifying each recipient that does not have a delivery preference that the message is available for retrieval.

100. A computer implemented method for sending a secure message to multiple recipients comprising:

encrypting a message;

sending the encrypted message to a forwarding server, including providing a list of recipients to the forwarding server;

at the forwarding server, decrypting the encrypted message and determining a decryption capability for each recipient in the list of recipients; and

for each recipient, re-encrypting the decrypted message according to the decryption capability of the recipient and delivering the re-encrypted message to the recipient.

101. The computer implemented method of claim 100, further comprising:

for each recipient that does not have decryption capability or the decryption capability cannot be determined, notifying the recipient that the message is available for retrieval.

102. The computer implemented method of claim 101, wherein:

notifying the recipient includes notifying the recipient that the message is available for retrieval through a secure link.

103. The computer implemented method of claim 100, wherein:

determining a decryption capability for each recipient includes determining whether each recipient has an associated published key.

104. The computer implemented method of claim 100, wherein:

determining a decryption capability for each recipient includes determining whether each recipient has an associated certificate.

105. The computer implemented method of claim 100, wherein:

determining the decryption capability of each recipient in the list of recipients includes selecting one decryption capability in accordance with a recipient's preference if the recipient has more than one decryption capability.

106. A computing system for providing secure message services for messages

addressed to multiple recipients, comprising:

a forwarding engine executing on a computer operable to:

receive an encrypted message and a list of recipients;

decrypt the encrypted message;

for each recipient in the list of recipients, determine whether the recipient has a decryption capability;

for each recipient with a decryption capability, re-encrypt the message according to the decryption capability of the recipient and deliver the re-encrypted message to the recipient; and

for each recipient that does not have a decryption capability, notify the recipient that the message is available for retrieval.

107. The computing system of claim 106, wherein the forwarding engine is operable to:

notify the recipient that the message is available for retrieval through a secure link.

## Evidence Appendix

None.

## Related Proceedings Appendix

None.